AIR UNIVERSITY

AIR WAR COLLEGE

Bureaucracy versus Bioterrorism

Countering a Globalized Threat

STEPHEN G. HOFFMAN
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No. 69
Maxwell Air Force Base, Alabama

October 2012

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **OCT 2012**	2. REPORT TYPE	3. DATES COVERED **00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE **Bureaucracy versus Bioterrorism: Countering a Globalized Threat**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Air War College,325 Chennault Circle,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**31**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

The Maxwell Papers are available electronically at the Air University Press website at http://aupress.au.af.mil.

Disclaimer

Bureaucracy versus Bioterrorism:

Countering a Globalized Threat

Lt Col Stephen G. Hoffman, USAF

Two things are certain—death and taxes! Or maybe just taxes. Scientists are attempting to cheat death with rapidly progressing technologies capable of constructing and manipulating life synthetically from basic chemical elements. While the advancing rates of capability in computing speed, genomics, synthetic biology, and nanotechnology have the potential to improve and lengthen life for all humans, they also enable biological weapons that can destroy wide swaths of humanity or attack specific groups of individuals. This confluence of technology is advancing at exponential rates and seems to have the advantage over the limited detection, protection, and treatment capabilities offered by a lumbering bureaucracy.

While human nature has not changed, rapidly advancing technology is providing new and novel biothreats to our adversaries. Globalization and the increasing availability of knowledge required to develop biothreats, coupled with declining computing costs, work together to dramatically increase the likelihood of biological weapon proliferation over the next 25 years. Given a future proliferation of biological weapons to terrorist groups, facilitated by globalization and rapidly increasing technological advancements, can a bureaucracy develop an effective network of countermeasures to bioterrorism?

Developing a network of credible countermeasures requires a consistent demonstration of intent to defeat bioterrorists backed by a viable capability. Intent to counter bioterrorism must be communicated to both potential terrorists, as well as to scientists who may be vulnerable to terrorist propaganda. Scientists considering facilitating terrorists with technical support needed to develop biological weapons may be deterred through professional pressure by their peers in the life science community. The medical profession has long had a concentration of knowledge which, if used wrongly, had the capacity of harming the very patient needing care. Even with this potentially dangerous information, trained medical personnel have developed a set of standards efficiently applied across their professional community. Perhaps the life sciences professions can increase acceptable behavior through adopting a similar ethic, code of standards, and self-policing professional community.

In addition to efforts to deter individuals through professional peer pressure, a credible network of countermeasures will include the ability to detect and attribute unacceptable activity. Scientists secretly working to develop biological weapons for terrorists may be further influenced to return to the mainstream if their work is detected and attributed to them directly. Attribution has the effect of removing anonymity from those bioterrorists who might otherwise believe they are impervious to

retribution. With removal of anonymity through increased attribution, rogue scientists may be influenced to stop their unprofessional behavior.

Finally, communicating intent to defeat bioterrorists rings hollow if there is no capability to deny the potential terrorists their desired end state or to coerce them with a believable expectation of punishment. Mitigating consequences of biological weapons is one way to deter would-be terrorists. A demonstrated ability to quickly react and counteract the effects of a biological weapon would remove the reward that a terrorist desires. Establishment of quick reaction teams capable of identifying the threat and developing treatment with use of nanotechnology for mass aerosol inoculation may show how the United States is serious about bioterrorism. Furthermore, mitigating consequences can also influence the terrorist on a personal level. That is, effective international law enforcement may increase the risk of incarceration in the same way a quick response team may reduce the reward of mass casualties. Effective development and enforcement of international law is the final aspect of a proposed network of countermeasures to aid bureaucracy in combating a future proliferation of biological weapons.

Confluence of Technologies

> *The convergence of nanotechnology with information technology, biology, and social sciences will reinforce discoveries and innovation . . . .*
>
> —Pres. George W. Bush

Definitions and Background

Three key developing technologies underlying the biothreat environment are genome sequencing, synthetic biology, and nanotechnology. The term genome refers to the complete library of information contained on an organism's deoxyribonucleic acid (DNA) or in the case of some viruses, ribonucleic acid (RNA). Both DNA and RNA are constructed with strands (single for RNA and usually double for DNA) of simple units called nucleotides which in their complete form are referred to as the genomic sequence. The second developing technology, synthetic biology, is "the design and construction of new biological parts, devices and systems [as well as] the redesign of existing, natural biological systems for useful purposes."[1] Funded largely through venture capital sources, leading life science experts have already made significant strides toward constructing living organisms synthetically from basic chemical elements. The third developing technology is nanotechnology. "Nanotechnology is a revolutionary technology, growing progressively from rudimentary nanostructures toward molecular nanosystems."[2] Nanotechnology is particularly useful in genomic mapping.

Genomic mapping or sequencing is the first step in identifying sections responsible for disease so that drugs to suppress or counteract

that section of the genome can be developed. Simple organisms typically have less complex genomes and higher order organisms have longer genome strands. “In 1990 an international, publicly funded effort, [called] the Human Genome Project, was launched to map and sequence human DNA and make the information freely available to the scientific community.”[3] The project was completed two years ahead of schedule in 2003, and the pace of growth in genome sequencing has continued to increase.

Second, synthetic biology has also seen rapid gains in development. “Synthetic [biology] comes in two broad classes. One uses unnatural molecules to reproduce emergent behaviours from natural biology, with the goal of creating artificial life. The other seeks interchangeable parts from natural biology to assemble into systems that function unnaturally.”[4] In July 2002 beginning only with a genomic sequence of a single strand RNA, researchers created and activated a virus identical in appearance and effect to naturally occurring polio.

The third technology impacting the biothreat environment is nanotechnology, which refers to development of capabilities by scientists to manufacture on a molecular level. A nanometer is one-billionth of a meter which is about five or 10 times as long as the width of an atom. “What is interesting about nanotechnology is that it functions as a technological multiplier.”[5] That is, nanotechnology is merely a facilitator of synthetic biology-providing tools and processes required to manipulate

genomic strands. A US Department of Agriculture report identifies detection of pathogens as one of many potential applications of nanotechnology.[6] Lawrence Berkeley National Laboratory scientists are capitalizing on the advancing rate of technology by developing "sensor systems that both detect nanoparticles and rely on the formation of nanoparticles that have been developed as sensing species."[7] Obviously, a strategy countering bioterrorism is further complicated by continuing advances in these areas.

Advancing Rate of Development

The rapid progress in genomics, synthetic biology, and nanotechnology has surprised many professionals in the life science fields; the overwhelming consensus is that the pace of advancement is likely to increase. Beneath all three of these technologies is the unmistakable linkage between increasingly powerful computers and advances in genomic sequencing, synthetic biology, and nanotechnology. The synergistic effect of technological advancement, coupled with increasingly powerful computers, offer incredible commercial returns on investment while simultaneously increasing the risk of biothreat proliferation.

Ray Kurzweil showed in *The Singularity is Near* how microprocessor clock speeds have followed an increasing exponential trend line doubling every three years since 1975, while over the same period microprocessor costs (per transistor cycle) have followed a

declining exponential trend line (fig. 1); cutting their costs in half every 1.1 years.[8]

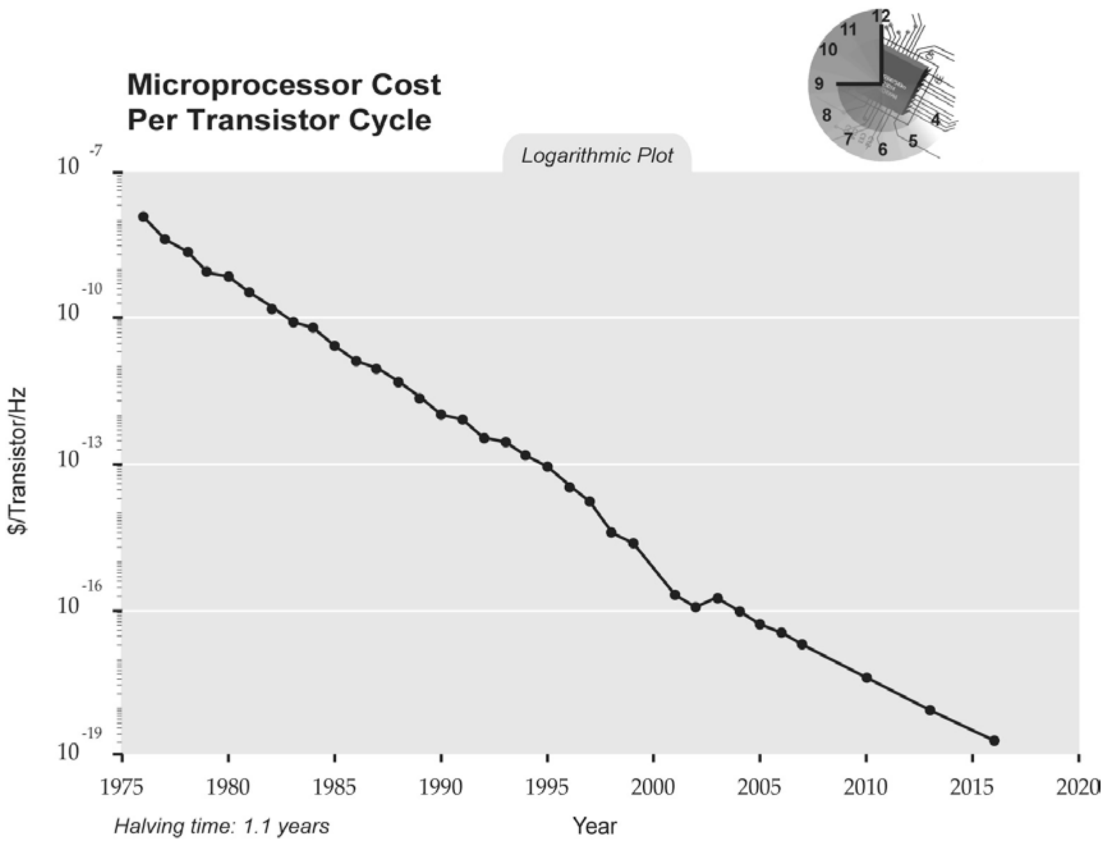

Figure 1. Microprocessor cost per transistor cycle. (Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology*, New York, NY: Viking Penguin Books, 2005, 61.)

This trend affects development of genomic and synthetic biology directly as both of these fields are dependent on powerful computers to process the enormous DNA sequencing code, and indirectly as a function of cost. That is, biotech companies are much more likely to receive venture capital where the cost-to-profit ratios are greatest.

Beginning in 1980 with the Human Genome Project, rates of increase in genomic sequencing and synthetic biology (fig. 2) appear to be following similarly explosive growth patterns. The Institute of Medicine

and National Research Council states, “[t]he accelerating pace of discovery in the life sciences has fundamentally altered the threat spectrum.”[9]

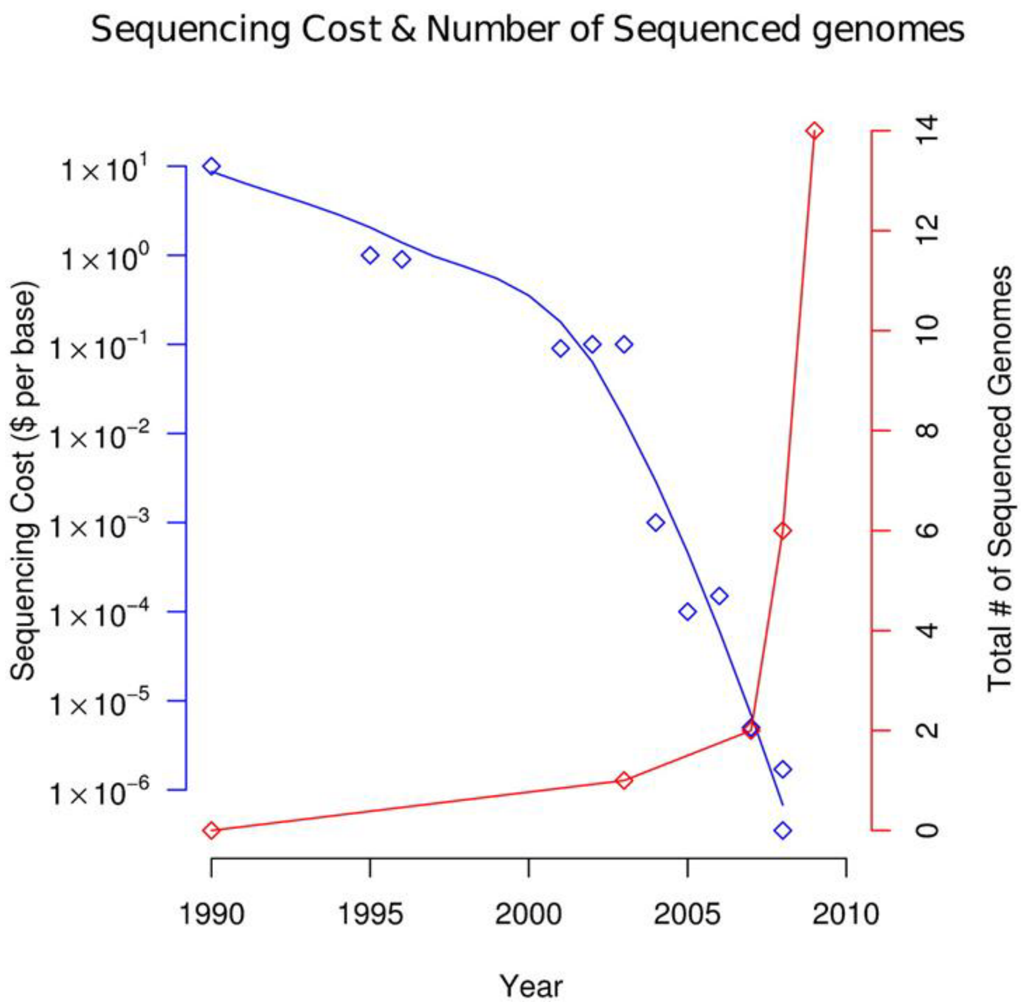

Figure 2. Sequencing cost and number of sequenced genomes. (Michael Snyder, Jiang Du, and Mark Gerstein, “Personal Genome Sequencing: Current Approaches and Challenges,” http://genesdev.cshlp.org/content/24/5/423.full, figure 1 [accessed 18 November 2010.])

The dramatic decrease of sequencing costs per pair of nucleotides is driven by two factors. First, the decreasing cost of computing power is making the hardware aspect of the process less expensive. Second,

software or process improvements that come as a result of scientific discovery raise the baseline across the industry. These two factors are complementary in that, as computing costs go down, more sequencing is being done by more companies; as the scientists at these companies learn, compete, and develop more efficient processes, the overall cost per sequenced genome pair plummets aggressively. Similar reasoning applies for why the total number of sequenced genes has rapidly increased. The economics of computing, genomics and synthetic biology show no sign of slowing.

A price performance curve for nanotechnology cannot be displayed in a manner similar to microprocessor costs, genomic sequencing costs, or number of sequenced genomes since nanotechnology refers to the molecular scale rather than a specific technology. Figure 3 does, however, indicate the rapidly increasing pace of US government funding for nanotechnologies across the first 10 years of this century. While the increase in funding has followed a relatively linear incline, the average annual increase over these 10 years is 23 percent. Cumulatively, this results in a 465 percent increase in federal funding for nanotechnology between 2000 and 2009.

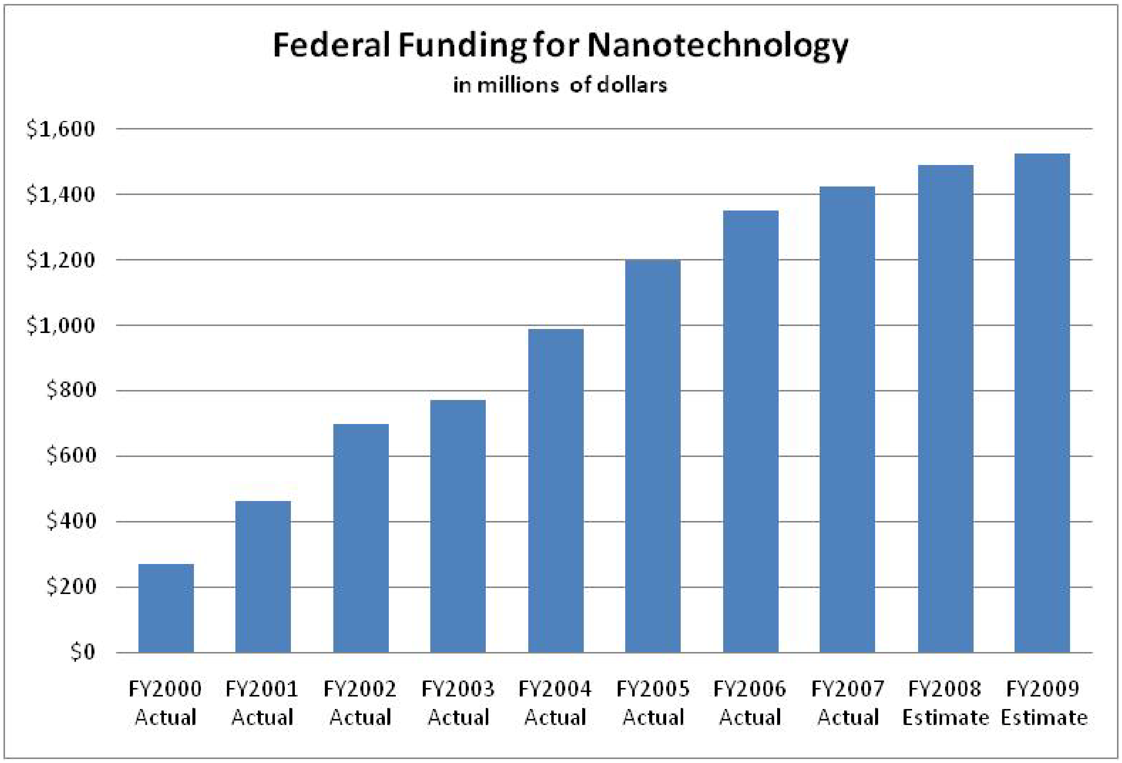

Figure 3. Nanotechnology funding, by agency: FY2001–FY2008 and FY2009 request. (John F. Sargent Jr., *The National Nanotechnology Initiative: Overview, Reauthorization, and Appropriation Issues*, Congressional Research Service [CSR] Report 7-5700, RL34401 [Washington DC, 6 May 2009], 16.

Given the austerity of federal funding over this period, an average annual increase of 23 percent is significant. Of course the federal government is not the only funding source for nanotechnology, but this data does emphasize the point that along with computing cost efficiencies, and genomic and synthetic biology advancements, nanotechnology enables exponentially growing advances in life sciences by facilitating smaller, cheaper and faster computing.

Shopping List for a Do-It-Yourself Bioterrorist

One consequence of increasingly cost efficient computing power coupled with advances in genomics, synthetic biology, and

nanotechnology is that do-it-yourself (DIY) genetic engineering is entering the realm of the possible. Barry Pallotta and Michael Finnin at the Institute for Defense Analyses detailed how DIY biologists can use everyday items (fig. 4) to attain rudimentary biological engineering capabilities.

Professional	Do-It-Yourself
Gel Electrophoresis	Drinking Straws, 9V Batteries, Food Grade Agar
Pipettor	Coffee Stirrer
Electroporator	Ultrasonic Jewelry Cleaner
Centrifuge	Dremel-Fuge, Coffee Grinder
Temperature Bath	Pot of Warm Water
PCR Thermocycler	3 Pots of Warm Water
Autoclave	Pressure Cooker
CO_2 Cell Incubator	CO_2 from Vinegar and Baking Soda
Enzymes and Solvents	Household Chemicals
Analytical Balance	Jewelry/ food Scale (mg Precision)

Figure 4. DIY biologist laboratory using household items. (Barry S. Pallotta and Michael S. Finnin, “DIY Biology: Capabilities Assessment” [internal study: CRP-2139, Institute for Defense Analyses, Alexandria, VA, for government use only, 4 May 2010], slide 9.)

With very little effort searching online auction sites such as eBay, the DIY biologists can greatly enhance their basement laboratories with a strikingly small financial investment. This proliferation of inexpensive technological hardware is an unexpected byproduct of globalization that offers alternatives to otherwise prohibitively expensive scientific

equipment, previously available only to universities and government organizations. Armed with only online access and $1,000, the DIY biologists can purchase professional equipment like the following recently advertised on eBay: temperature bath–$150, cell incubator–$230, PCT thermocycler–$200, and centrifuge–$100.

There are, however, limits to the DIY biologists as their learning and capabilities are only facilitated by the successes of the professional biomedical community. The DIY community has achieved only level three, of the nine levels of technical complexity (fig. 5), while PhD level professionals in the biomedical community have achieved level seven. Even though the capabilities of DIY biologists are significantly lower than the professional community, technical advances are making this a viable concern for the future. The potential damage of malicious or accidental biological pathogen release by biologists outside the professional community is becoming more likely with the proliferation of inexpensive technology.

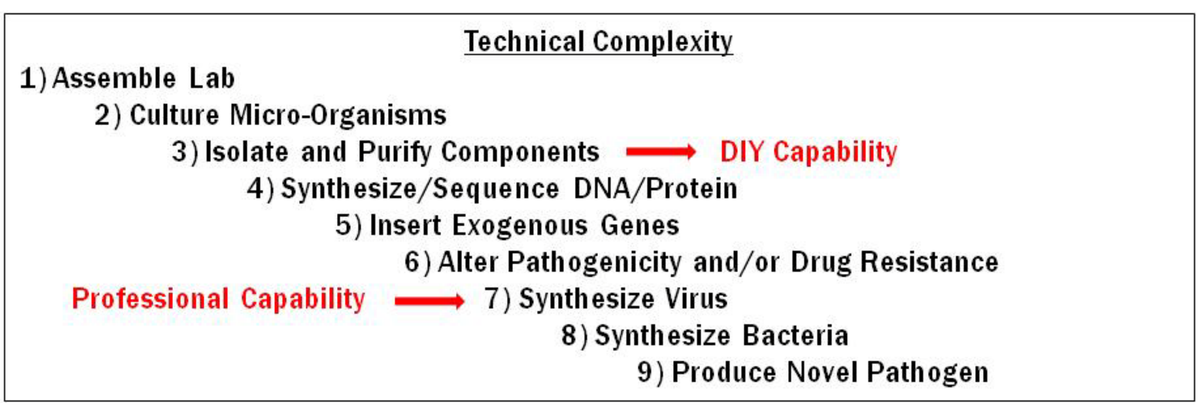

Figure 5. Biocapability technical complexity levels 1–9. (Pallotta and Finnin, "DIY Biology: Capabilities Assessment," slide 17.)

The DIY community has yet to independently sequence or synthesize DNA similar to results of the Human Genome Project (1990–2003). Following the successful Human Genome Project, the professional community compiled numerous additional successes for the following eight years (2003–11), culminating in viral synthesis. While the professional community required 13 years to sequence DNA and eight additional years to synthesize a virus, the DIY community benefits from a dispersion of knowledge through published scientific reports. Estimating (very conservatively) a 10–20 year lag behind the professional community, DIY biologists are likely to obtain technical complexity level seven or eight by 2035. Given the advancing pace of development across genomics, synthetic biology, and nanotechnology, an estimated technical complexity level nine for the DIY community is not at all unreasonable. Failure of bureaucracy to develop a novel network of countermeasures against DIY scientists and would-be bioterrorists, who can wage warfare from Wal-Mart, is foolhardy.

What Failure Looks Like

Globalization and the Internet have enabled widespread distribution of technical knowledge and hardware, and there is no way to put the genie back in the bottle. Relying solely on traditional deterrent policies against a globally proliferated biothreat will not suffice when attempting to counter a technology-empowered bioterrorist. If the bureaucracy can ever hope to develop an effective network of

countermeasures to bioterrorism, then certainly the first step in that development is an accurate assessment of the consequences of what failing to do so would have on the United States. Andrew Krepinevich, in the “Pandemic” chapter of his 2009 book, *7 Deadly Scenarios*, provides a glimpse of how that failure might look.

> Meanwhile, as the United States increasingly resembles a vast collection of semi-ghost towns, to the south literally millions of peoples are on the move. . . . This mass of Mexicans, now estimated at nearly eight million, has no organizing force directing it, yet all its participants are unified toward one goal: crossing the border into the United States, in hope of gaining access to this country’s medical system—which ironically in many ways has simply ceased functioning in any meaningful way. This mass migration is . . . driving Mexico’s population north—a human tidal wave about to crash across America’s borders.[10]

A bioterrorist attack on the United States could take the form of an introduction of a mutated avian flu virus, capable of being passed human-to-human into unsanitary villages in Mexico. Poor surveillance by the World Health Organization, coupled with typical American disbelief of vulnerability to a pandemic, would likely permit early reports of 10, 20, or 50 deaths scattered across Mexican villages to go largely unnoticed in the United States. One characteristic of viral growth is its exponential increase, so these seemingly small and scattered deaths could, within weeks, ramp into millions of cases of avian flu. Even though the Spanish influenza of 1918 killed 675,000 Americans and estimates of an avian flu pandemic are that 2,000,000 could die, the

Center for Disease Control (CDC) has failed to develop sufficient antivirus stockpiles.

"The combination of the pandemic, the lack of government preparedness, and sensationalist media [would diminish American's] confidence and trust in their government."[11] Furthermore, the second and third order effects of a pandemic, coupled with global mobility, may be increased gang activity, looting, and violent crime worldwide such that implementation of martial law may be required. Overwhelmed governments may attempt to clamp down on individual rights to free speech and assembly if mob violence were to spontaneously erupt anywhere social networks indicated medical supplies existed. In the United States, the president could nationalize all antiviral treatments under the direction of the CDC, Federal Emergency Management Agency and the Department of Defense. Since "95 percent of the world's vaccine is produced by countries comprising only about 10 percent of the world's population,"[12] minority groups may characterize the president's nationalization of medical supplies as nothing more than opportunistic ethnic cleansing. In light of these global implications to bioterrorism, it is imperative that the United States show leadership in propagating ethical norms of responsible conduct.

Reinforcing Norms of Responsible Conduct

> *We will work with domestic and international partners to protect against biological threats by promoting global health security and reinforcing norms of safe and responsible conduct; . . . expanding our capability to prevent, attribute, and apprehend those who carry out [bio]attacks.*
>
> —Pres. Barack Obama

Police within Profession

The education, training, and skills of scientists in biology, chemistry, and genetics empower life science professionals with capabilities that must be used according ethical standards of professional peer organizations. Pledging an oath to publically state one's agreement and voluntary self-censorship according to the guidelines of the group's ethical standards is an effective way of bonding a member to his or her profession. The very word "profession" in its Latin origin means "bound by an oath."[13]

"Nearly all medical schools incorporate some form of professional medical oath into their graduation ceremonies. The oldest and most popular of these oaths is the Hippocratic oath, composed more than 2,400 years ago."[14] In addition to medical doctors, oaths have been adopted in many other professions to build a commitment to the group which encourages and polices ethical actions. When these oaths are additionally printed and signed, there is an even greater level of buy-in on the part of the member. Individuals who profess such an oath are

motivated primarily by altruistic desires, but negative reinforcement from peer reproach also encourages proper behavior.

Additionally, the professional communities to which members pledge an oath provide tangible value to those members in the form of certification and peer recognition. The very nature of professions with unique education and training necessitates a very precise vernacular not often understood by the layman. When a member demonstrates proficiency through testing or peer review, a certification may be granted, externally validating this member. While outsiders may not understand the particular language or nuances of the profession, certification is often sufficient for promotion or advancement. It follows then that potential loss of a professional certification may also act as a deterrent to unapproved activity.

Due to the danger of globalized technological advancements in the life sciences arena, even peer review may be insufficient to safeguard against biothreats. “Sir Joseph Rotblat, the 1995 Nobel Peace Prize laureate, urged in his acceptance speech that ‘the time has come to formulate guidelines for the ethical conduct of scientists, perhaps in the form of a voluntary Hippocratic Oath’.”[15] Developing and implementing guidelines in the form of an oath would help fulfill President Obama’s mandate of protecting against biothreats while “reinforcing norms of safe and responsible conduct.”[16]

There are limitations, however, to the effectiveness of professional policing. Western professionals are motivated to ethical activity through a compelling system of reward and punishment from a linear-active society that places great value on both words and deeds. Societies valuing tribal, ethnic, or religious relationships more highly than ethical codes will not provide the ethical underpinning necessary for professional policing. Therefore, a second capability must be added to the proposed bureaucratic network against bioterrorism—increased attribution to find and expose those who do not follow the professional code.

Increase Attribution

Detection of bioterrorism is a collective activity heavily dependent on physical evidence acquired through material sensors, whereas attribution demands a higher level of effort as both capacity and intent must be shown. Detection is the tool for validating enemy capacity toward biothreat development, testing, or use. Attribution demands evidence that not only is there an adversary involved in some stage of biothreat activity, but that that adversary also intends to use that biothreat as a weapon. Researchers at University of Florida are developing a nanotechnology that may aid with both detection and attribution, providing at least one avenue toward removing anonymity. These researchers are developing a "smart dust" that changes color when exposed to precursor elements of biological weapons.[17]

Attribution can continue to be an effective aspect of the national security strategy even for individual bioterrorists if the strategy is applied with understanding from the perspective of the adversary. Deterrence through attribution requires the capability to detect and attribute bioterrorist activity coupled with credibility to deny or punish adversaries' efforts. Attribution has the effect of removing anonymity from bioterrorists who might otherwise believe they are impervious to retribution. An experiment validating this conclusion by psychologists Chen-Bo Zhong, Vanessa Bohns, and Francesca Grino showed how volunteers in a dimly lit room were decidedly more likely to lie, cheat, and steal than volunteers in a brightly lit room. In this experiment, darkness provided the anonymity which facilitated criminal activity.[18]

Use of smart dust as a nanotaggant may, as an example, serve as a means of removing anonymity of those working with precursor elements of biological weapons. That is, a rogue scientist experimenting with the building blocks of biological weapons may be deterred from further effort if his tools, workplace, hands, and clothing all fluoresce—letting the scientist know that he or she is not as anonymous as he or she may have thought. Should the color-changing smart dust not deter the wayward scientist, then policing from the professional community may discourage continued development of biological weapons.

A broad array of collection tools and techniques add flexibility to detection capabilities which, in turn, enhances the ability to attribute

developing threats from would-be bioterrorists. In cases where both loss of anonymity and professional policing fail to dissuade rogue scientists, then the use of nanoparticles may mitigate the consequences as tagging identifiers for criminal apprehension and prosecution. Mitigation of consequences is the third capability necessary for the proposed bureaucratic network against bioterrorism. This capability is comprised of a two-prong effort to counter bioterror activity—effective counteraction of biothreats and technology enhanced enforcement of international law.

Mitigate Consequences

Aggressively working to mitigate the consequences of a bioterrorist act may deter the act in the first place. One method of mitigating consequences is to develop quick response teams with the proper training and expertise to rapidly counter the effects of a biological weapon. Three essential capabilities of such a quick response team are the ability to: (1) rapidly identify a pathogen used in a bioattack; (2) develop an effective treatment; and (3) administer treatment and inoculation to the appropriate populations. Quick response teams would mitigate the terrorist's desired reward of causing mass American casualties. Additional mitigation may result through achieving an increased likelihood of capture and punishment to the potential bioterrorist through improved international law and treaties pertaining to life sciences.

Key technologies essential to a quick response team are nanovector therapy and nanosurface technology. In nanovector therapy, an ideal drug dosage is delivered at full concentration to the intended tissue only. This optimal method of delivery reduces the amount of drug required for treatment while diminishing undesired side effects in tissue or organs where the drug is unnecessary but might have been absorbed. Another benefit to the efficacy of this style of drug delivery is that the body's natural defenses can be purposefully bypassed, further reducing collateral damage.[19] This technique is partially made possible by nanosurface technologies where drug treatments are covered by protective nanocoatings. The nanosurface technology enables application of coatings that are programmable to dissolve when and where desired. This technique is an adaptation of a naturally occurring coating where pathogens or germs are either repelled or attracted based on the host organisms requirement.

While these nanotechnologies are still in development, their utility to quick response teams would be invaluable in identifying, treating, and inoculating against a biothreat. Using nanotechnology is a necessary technique if any bureaucracy hopes to keep pace with rapidly advancing technologies. Linear thinking about medical treatment delivery will not suffice when adversaries demonstrate a willingness to use every nonlinear attack technique at their disposal. That is, preparations must be made to dispense care using nanotechnologies in a very short period

of time with mass aerosol delivery of nanosurface encapsulated antibiotics or inoculation to effectively mitigate a terrorist's desired outcome. Nanotechnologies may even aid in improved international law application through single molecule detecting sensors. If smart dust nanosensors were available in the hunt for forensic evidence of a bioterrorist act, this smart dust may actually deter terrorism through increased risk of capture and punishment.

Recommended Additional Air Force Study

The Air Force can contribute to President Obama's biothreat strategy through increased emphasis on attribution and detection. Therefore, technological developments in genomics, synthetic biology, and nanotechnology will be important as the Air Force strives to fully understand the capability and intent of US adversaries; and when punitive actions are necessary, use of nanotaggant identifiers for targeting of kinetic weapons. There are, however, a few unanswered questions about pragmatic implementation of a bureaucratic network of biothreat countermeasures.

How Many Life Science Officers are Enough?

As of January 2010, the total number of active duty officers in the Air Force was 65,515 with only 108 (or .17 percent) identified as biologists or chemists. These scientists were assigned primarily to acquisition organizations supporting programs instrumental to development of biological weapon analysis or detection tools. Near-term

increases in life sciences personnel resources may contribute significantly toward leading-edge detection capabilities facilitated by the same technology that is increasing biothreat likelihood. While .17 percent of all active duty officers trained and employed as life scientists seems paltry, the correct number of truly necessary life science officers is currently unknown. A full investigation of the life sciences personnel requirement is recommended to determine the appropriate number of chemists and biologists required in the scientist officer core.

How Should Information Cross-Flow Occur?

Acquisition and intelligence units currently have no mandated flow of information ensuring the scientific efforts to improve biocollection are broadly included into future acquisition programs. Likewise, there is no institutionalized flow of information from medical officers to the intelligence and acquisition communities to capitalize on their knowledge of medically related advances in synthetic biology. Developing a mechanism for cross-functional communication between the intelligence, medical, scientific, and acquisition communities may increase the likelihood that the latest developments in life science fields are relayed back to acquisition program offices. Institutionalizing this feedback may also formalize the communication with the goal of ensuring the most relevant detection techniques are considered for incorporation into developing programs. It is recommended that the intelligence, acquisition, medical, and scientific career fields' functional communities

investigate an institutionalized cross-flow mechanism for efficient distribution of the most current life science information.

Is Life Science Certification Necessary?

All three aspects of the proposed network of countermeasures—professional policing, increasing attribution, and consequence mitigation—may be facilitated by a well-documented professional life science community. In some instances, scientists may self-police if they believe a sanctioning body might remove a professional license if they are caught breaking an ethical code or professional oath. An increased awareness of scientists' professional activity, resulting from a certification process, may increase attribution capabilities. Additionally, international life science laws and treaties may be more effectively enforced by a cadre of externally certified life science professionals. It is therefore recommended that an industry-accepted certification plan for life sciences officers be developed and implemented.

Conclusion—A Network of Countermeasures

Genetics, synthetic biology, and nanotechnology are established technologies that have shown incredible rates of advancement. These rates of advancement in the life sciences are anticipated to accelerate even faster, facilitating further developments which make proliferation of biological threats by 2035 almost certain. However, even in a future where biological weapons are proliferated to terrorists through

globalization and technological advancements, a bureaucracy can develop an effective network of countermeasures to bioterrorism.

The first aspect of this network is professional policing among life science professionals through development of an oath of ethical actions. A life science oath would “reinforce norms of safe and responsible conduct”[20] while creating ethical standards within the profession. The second aspect in this network is a nanotechnology detection capability to permit unambiguous attribution of bioterrorist activity. For example, this attribution capability may strip anonymity from bioterrorists and coerce them toward civil behavior through the use of fluorescing nanotaggants. Knowledge of terrorist actions, once communicated in the light of day, will increase American credibility and deterrent effectiveness through either denial or punishment. The third aspect of this network is mitigation of the consequences of terrorists’ desires though development of quick response teams capable of rapidly identifying pathogens, treating the infected, and inoculating the masses through nanovector delivery techniques. Through the use of nanotechnology and improved implementation of international life science laws and treaties, an increased likelihood of punishment to bioterrorists may be realized. Neither the reduction of reward nor increase of risk must be perfect; merely disincentivizing the economics of biological weapon use may discourage would-be terrorists from investing effort in this area.

Developing this network of countermeasures will allow the US bureaucracy to combat bioterrorism by transforming some scientific competitors into collaborators through professional policing. Those who cannot be co-opted by peer pressure may be deterred through a removal of anonymity brought about with technologically enhanced detection and attribution. Finally, bioterrorists undeterred by the loss of anonymity may be compelled to halt their behavior through a two-pronged effort to mitigate biothreat consequences. This consequence mitigation effort would: (1) decrease a terrorist's motivation by developing quick response teams capable of preventing mass American casualties with nanovector treatment and inoculation; and (2) increase the terrorist's personal jeopardy through nanotechnology-enhanced international law enforcement.

Effective Air Force participation in this proposed bureaucratic network of countermeasures requires a few foundational questions be answered. To reduce risks of a 2035 biothreat and better support the 2010 National Security Strategy, the Air Force must (1) determine the proper level of scientific personnel required; (2) institutionalize cross-functional communication across the intelligence, scientific, acquisition, and medical functional communities; and (3) develop an industry-accepted certification program for life science officers. Amid a rapidly changing technological environment, accomplishing these actions now will decrease future risk in the president's overall biothreat strategy by

systematically increasing American credibility, capability, and communication.

Notes

---

1. Synthetic Biology, http://syntheticbiology.org/ (accessed 27 September 2010).

2. David M. Burube, *Nano-Hype: The Truth Behind The Nanotechnology Buzz* (Amherst, NY: Prometheus Books, 2006), 17.

3. John Sulston and Georgina Ferry, *The Common Thread: A Story of Science, Politics, Ethics, and the Human Genome* (Washington, DC: Joseph Henry Press, 2002), viii.

4. Steven A. Brenner and A. Michael Sismour, “Synthetic Biology,” *Nature Reviews: Genetics* 6, no. 6 (July 2005): 533.

5. Burube, *Nano-Hype*, 22.

6. Ibid., 193.

7. Sensors Group, Lawrence Berkeley National Laboratory, “Nanoparticle Sensors and Nanoparticle-Based Detector Systems,” http://sensors.lbl.gov/sf_nano.html (accessed December 2010).

8. Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology* (New York, NY: Viking Penguin Books, 2005), 61–62.

9. Institute of Medicine and National Research Council of the National Academies, *Globalization, Biosecurity, and the Future of Life Sciences* (Washington DC: The National Academies Press, 2006), 5.

10. Andrew F. Krepinevich, *Seven Deadly Scenarios: A Military Futurist Explores War in the 21st Century* (New York, NY: Bantam Dell, 2009), 92.

11. Ibid., 99.

12. Ibid., 113.

13. Daniel Fu-Chang Tsai and Ding-Shinn Chen, “An Oath for Bioscientists,” *Journal of Biomedical Science*, 2003, http://www.ncbi.nlm.nih.gov/pubmed/14576458 (accessed 18 November 2010), 571.

14. Raphael Hulkower, “The History of the Hippocratic Oath: Outdated, Inauthentic, and Yet Still Relevant,” *The Einstein Journal of Biology and Medicine* 25 and 26, no. 1 (2009–10): 41.

15. Tsai and Chen, “An Oath for Bioscientists,” 569.

16. Pres. Barack Obama, *National Security Strategy,* 24.

17. Lynn E. Foster, *Nanotechnology: Science, Innovation, and Opportunity* (Upper Saddle River, NJ: Prentice Hall, 2006), 218.

18. Chen-Bo Zhong, Vanessa K. Bohns, and Francesca Gino, “Good Lamps Are the Best Police: Darkness Increases Dishonesty and Self-Interested Behavior,” *Psychological Science*, 29 January 2010, http://pss.sagepub.com/content/early/2010/01/28/095679760936075 4.abstract (accessed 18 November 2010).

19. M. Farrari, “Nanovector Therapeutics,” *Current Opinion in Chemical Biology*, August 2005,

http://www.ncbi.nlm.nih.gov/pubmed/15967706 (accessed 18 November 2010).

20. Obama, *National Security Strategy*, 24.